(12) UK Patent Application (19) GB (11) 2 402 852 (13) A

(43) Date of A Publication 15.12.2004

(21) Application No: 0412786.6

(22) Date of Filing: 09.06.2004

(30) Priority Data:
(31) 0313663 (32) 13.06.2003 (33) GB

(71) Applicant(s):
Hewlett-Packard Development Company L.P.
20555 S.H.249, Houston, Texas 77070,
United States of America

(72) Inventor(s):
Liqun Chen
Keith Alexander Harrison

(74) Agent and/or Address for Service:
Hewlett-Packard Limited
Intellectual Property Section, Building 3,
Filton Road, Stoke Gifford, BRISTOL,
BS34 8QZ, United Kingdom

(51) INT CL[7]:
H04L 9/00 9/30 9/32 29/06

(52) UK CL (Edition W ):
H4P PPEB

(56) Documents Cited:
WO 2003/073713 A1 WO 2003/017559 A2
US 6275936 B1
http://pollux.usc.edu/~xuhuad/publications/wisa.pdf, "Identity-based mediated RSA", D. Boneh, X. Ding & G. Tsudik, 3rd International Workshop on Information and Security Applications (WISA'02), Jeju Island, Korea, 2002
http://www.hpl.hp.com/techreports/2003/HPL-2003-101.pdf, "IBE applied to privacy and identity management", Marco Casassa Mont and Pete Bramhall, HP Labs Technical Reports, last modified 02/06/2003

(continued on next page)

(54) Abstract Title: **Mediated RSA cryptographic method and system using blinding**

(57) A mediated RSA cryptographic method and system is provided in which a sender (10) encrypts a message (m) using an encryption exponent e and a public modulus n, and a recipient (20) and a trusted authority (50) cooperate with each other to decrypt the encrypted message by using respective components $d_U$, $d_T$ of a decryption exponent. In order to prevent the trusted authority (50) from reading the message in the event that it has access to the recipient decryption exponent components $d_U$, the recipient (20) blinds the encrypted message before passing it to the trusted authority (50). This blinding is effected by a modulo-n blinding operation using a factor $r^e$ where r is a secret random number. The trusted authority (50) then applies its decryption exponent component $d_T$ to the message and returns the result to the recipient (20) who cancels the blinding and applies its decryption exponent component $d_U$ to recover the message. In a preferred embodiment, the encryption exponent is based on a string (STR) comprising one or more conditions; this string is passed to the trusted authority (50) along with the blinded message and the trusted authority checks that the or each condition is satisfied before it determines and applies the appropriate decryption exponent component $d_T$. In a further embodiment the encryption exponent is based on a string chosen by the sender such that identifier-based mediated RSA is performed.

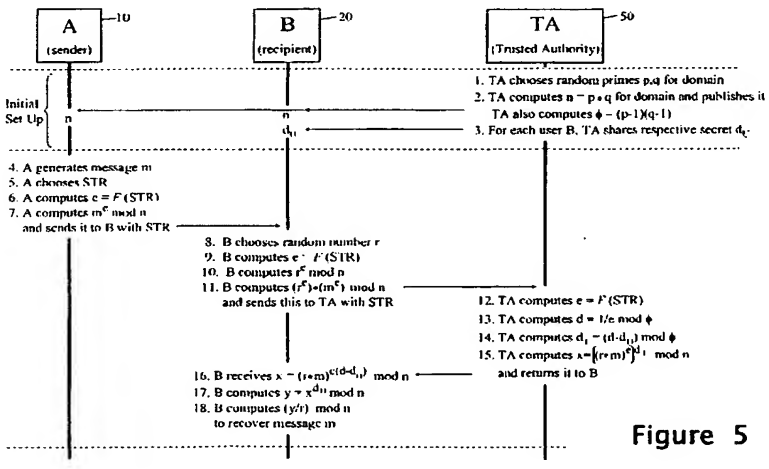
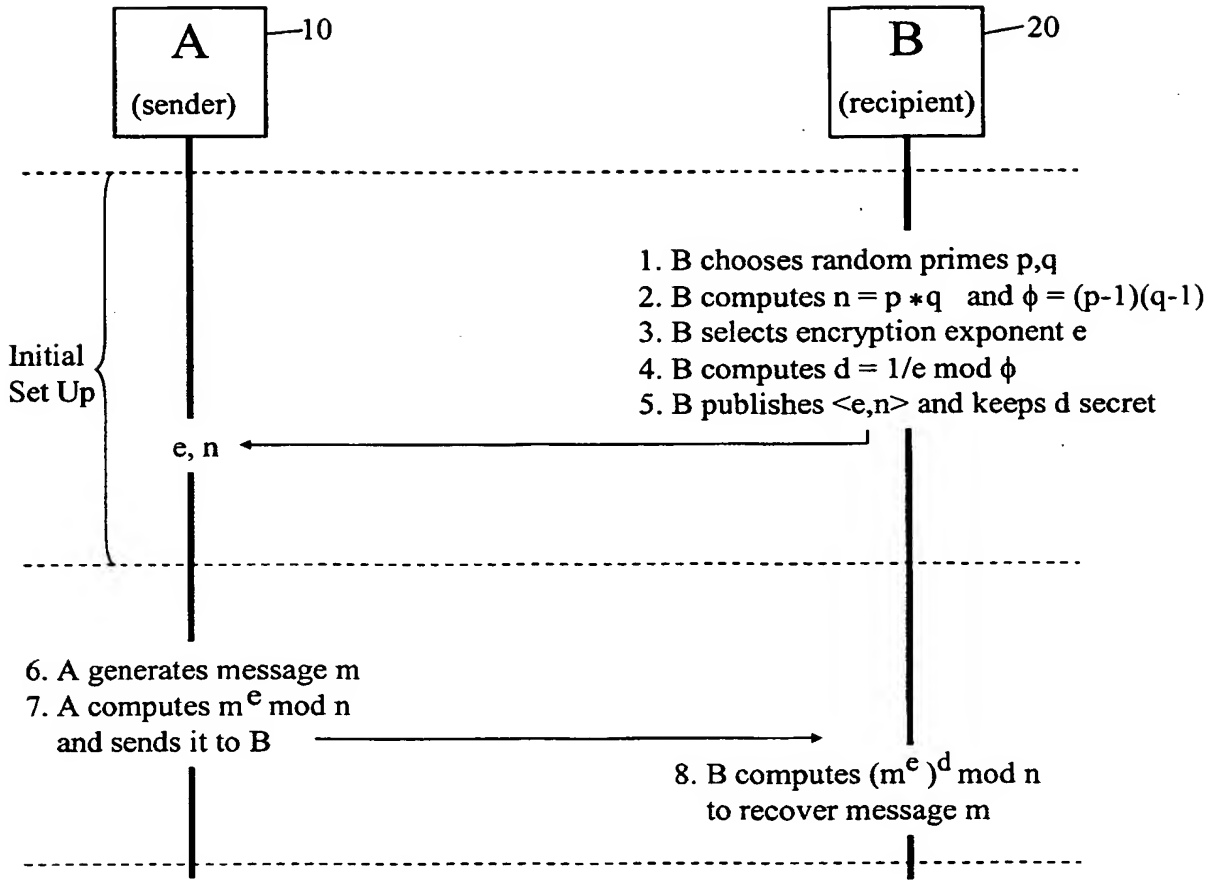



Figure 5

GB 2 402 852 A

(56) cont
**"A blind signature scheme based on ElGamal signature", Mohammed, E.; Emarah, A.E.; El-Shennawy, K., EUROCOMM 2000, Information Systems for Enhanced Public Safety and Security, IEEE/AFCEA , 17 May 2000, pp 51-53**
**http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C82/19 9.PDF, "Blind signatures for untraceable payments", Advances in Cryptology, Crypto >82, D. Chaum, pp199-203**

(58) Field of Search:
UK CL (Edition W ) **H4P**
INT CL[7] **G07F, H04L**
Other:




***Basic RSA***

**Figure 1**

(Prior Art)

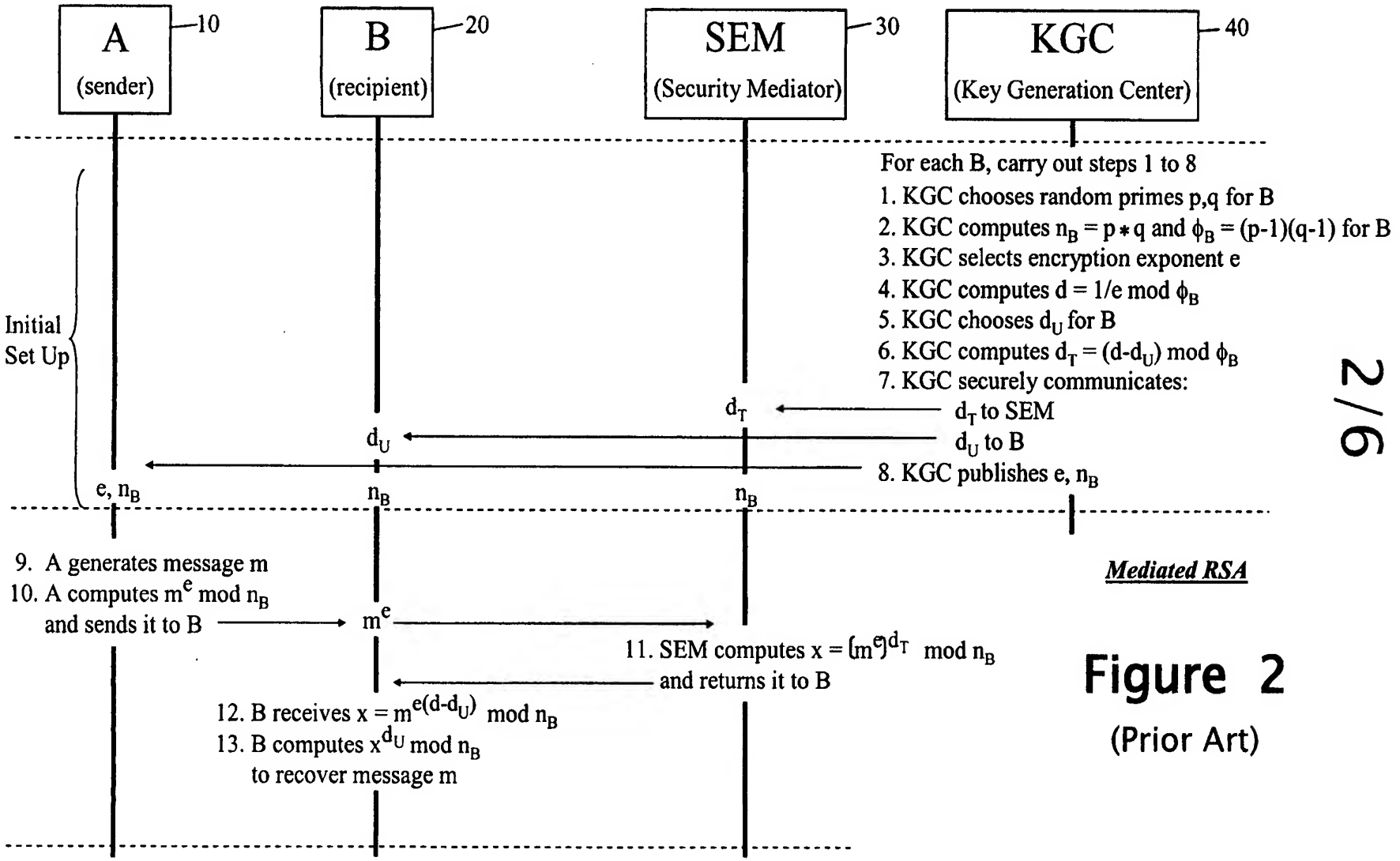
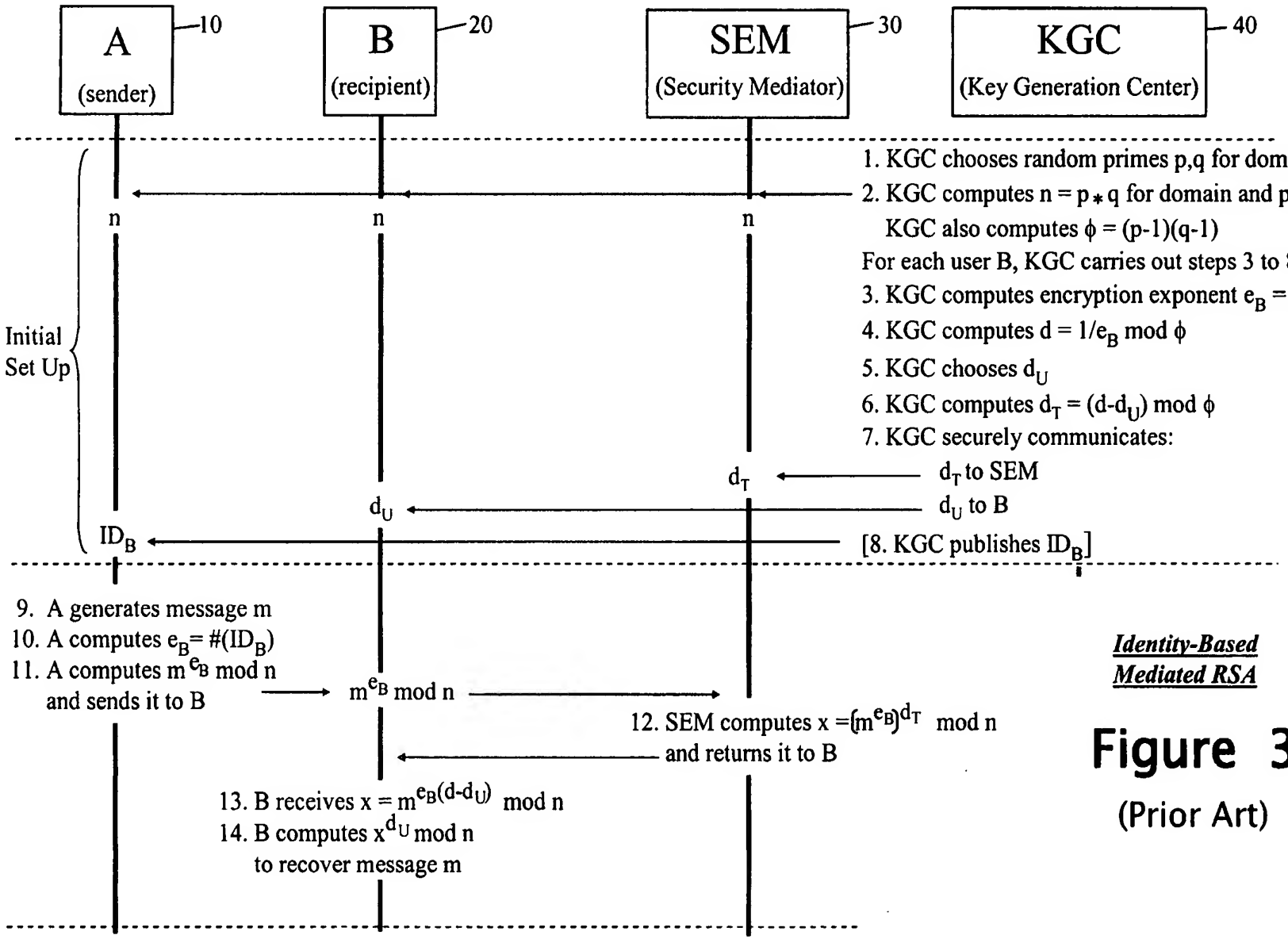



Figure 2

(Prior Art)




***Identity-Based Mediated RSA***

**Figure 3**

(Prior Art)

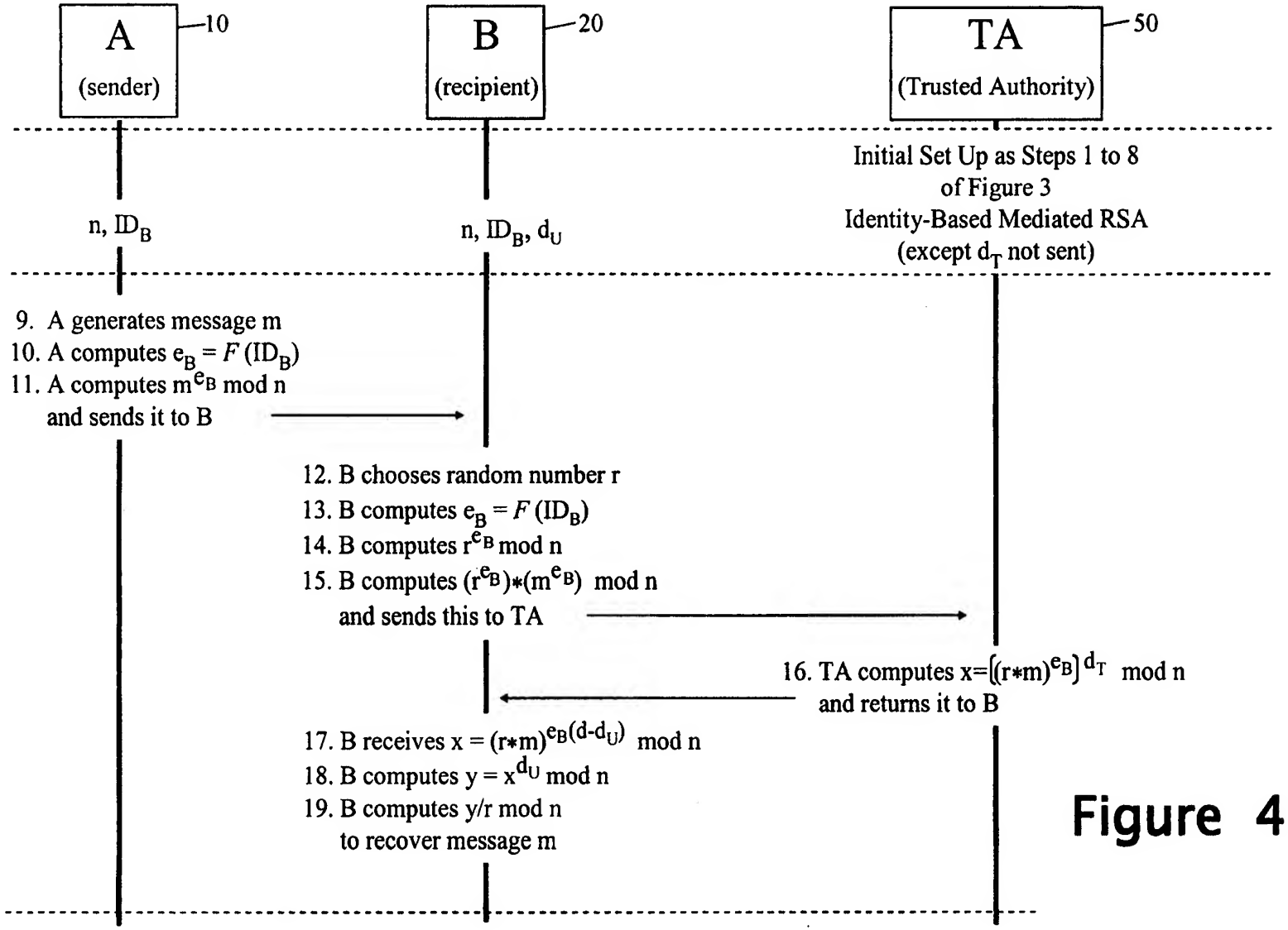

A
(sender)
10
B
(recipient)
20
TA
(Trusted Authority)
50
Initial Set Up as Steps 1 to 8
of Figure 3
Identity-Based Mediated RSA
(except $d_T$ not sent)
n, $ID_B$
n, $ID_B$, $d_U$
9. A generates message m
10. A computes $e_B = F(ID_B)$
11. A computes $m^{e_B} \bmod n$
and sends it to B
12. B chooses random number r
13. B computes $e_B = F(ID_B)$
14. B computes $r^{e_B} \bmod n$
15. B computes $(r^{e_B})*(m^{e_B}) \bmod n$
and sends this to TA
16. TA computes $x=[(r*m)^{e_B}]^{d_T} \bmod n$
and returns it to B
17. B receives $x = (r*m)^{e_B(d-d_U)} \bmod n$
18. B computes $y = x^{d_U} \bmod n$
19. B computes y/r mod n
to recover message m

Figure 4

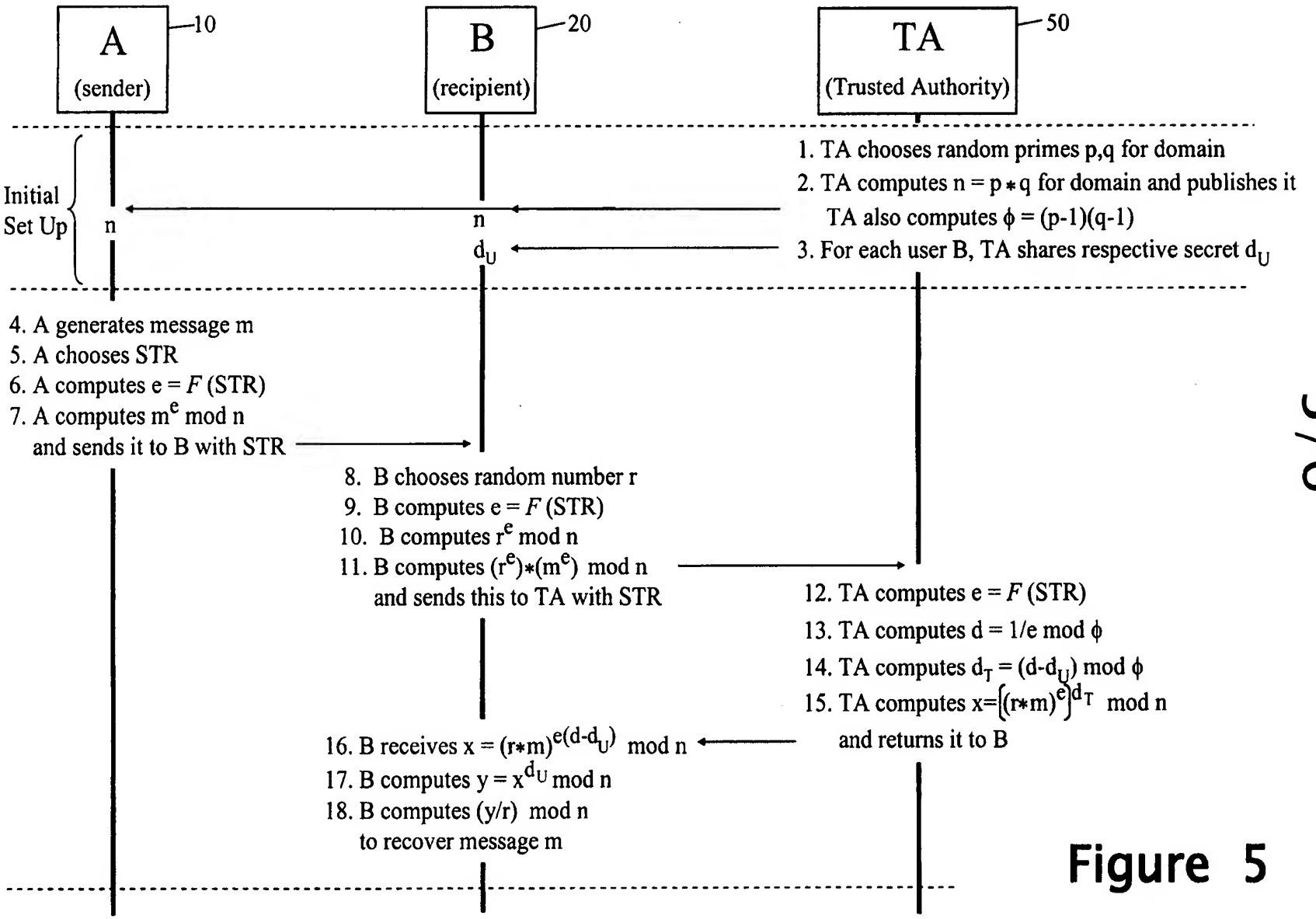

A
(sender)
10
B
(recipient)
20
TA
(Trusted Authority)
50
Initial
Set Up
n
n
$d_U$
1. TA chooses random primes p,q for domain
2. TA computes n = p * q for domain and publishes it
TA also computes $\phi = (p-1)(q-1)$
3. For each user B, TA shares respective secret $d_U$
4. A generates message m
5. A chooses STR
6. A computes e = *F* (STR)
7. A computes $m^e$ mod n
and sends it to B with STR
8. B chooses random number r
9. B computes e = *F* (STR)
10. B computes $r^e$ mod n
11. B computes $(r^e)*(m^e)$ mod n
and sends this to TA with STR
12. TA computes e = *F* (STR)
13. TA computes d = 1/e mod $\phi$
14. TA computes $d_T = (d-d_U)$ mod $\phi$
15. TA computes $x=\left[(r*m)^e\right]^{d_T}$ mod n
and returns it to B
16. B receives $x = (r*m)^{e(d-d_U)}$ mod n
17. B computes $y = x^{d_U}$ mod n
18. B computes (y/r) mod n
to recover message m

Figure 5

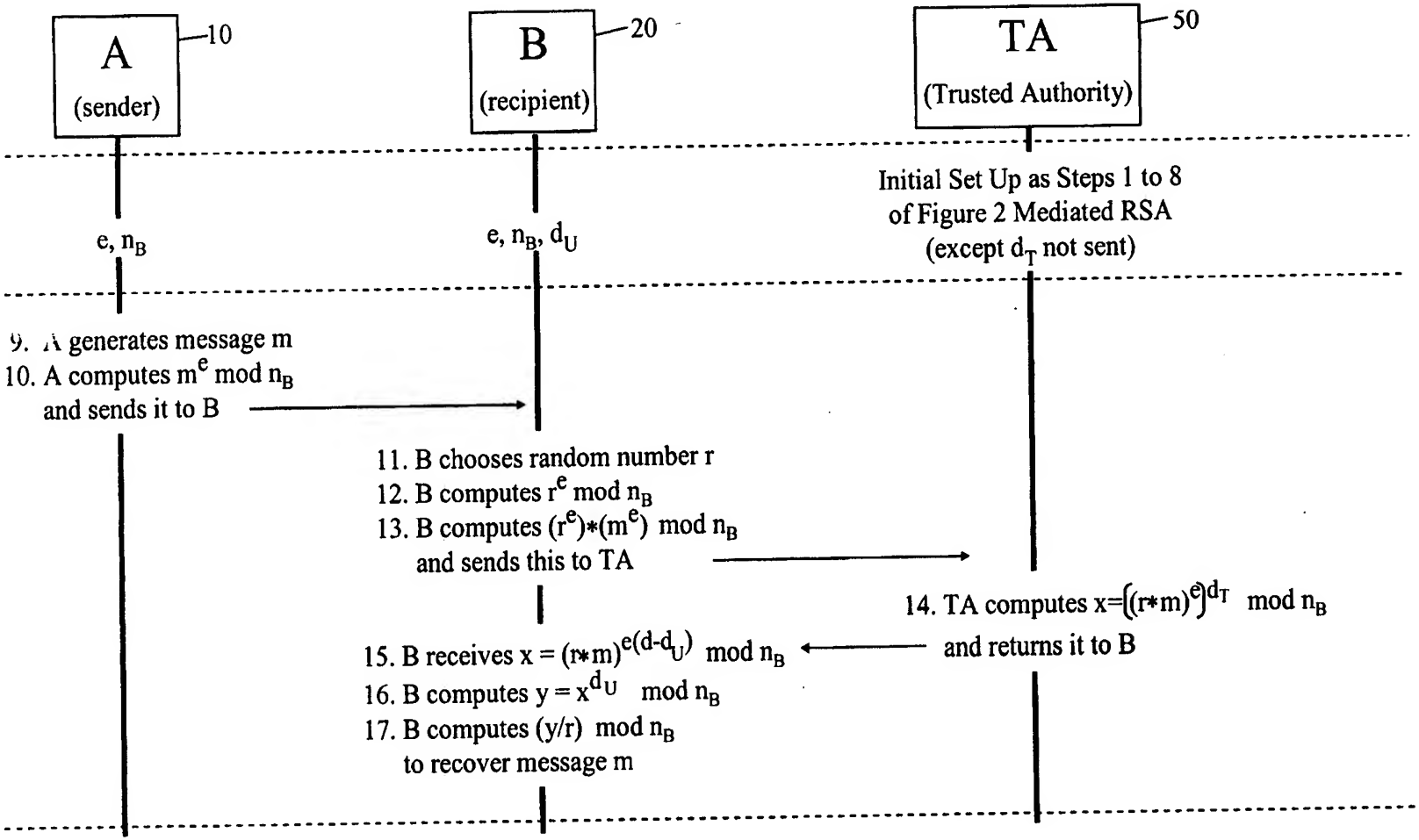

A
(sender)
10
B
(recipient)
20
TA
(Trusted Authority)
50
Initial Set Up as Steps 1 to 8
of Figure 2 Mediated RSA
(except $d_T$ not sent)
e, $n_B$
e, $n_B$, $d_U$
9. A generates message m
10. A computes $m^e$ mod $n_B$
and sends it to B
11. B chooses random number r
12. B computes $r^e$ mod $n_B$
13. B computes $(r^e)*(m^e)$ mod $n_B$
and sends this to TA
14. TA computes $x=[(r*m)^e]^{d_T}$ mod $n_B$
and returns it to B
15. B receives $x = (r*m)^{e(d-d_U)}$ mod $n_B$
16. B computes $y = x^{d_U}$ mod $n_B$
17. B computes (y/r) mod $n_B$
to recover message m

Figure 6

# Mediated RSA Cryptographic Method and System

## Field of the Invention

The present invention relates to a mediated cryptographic method and system.

## Background of the Invention

The RSA public key cryptographic method is well known and in its basic form is a two-party method in which a first party generates a public/private key pair and a second party uses the first party's public key to encrypt messages for sending to the first party, the latter then using its private key to decrypt the messages. More particularly, and with reference to Figure 1 of the accompanying drawings, in the basic RSA encryption method the following operational steps are carried out by a message sender A and a message recipient B acting through respective computing entities 10 and 20:

*Initial Set Up Phase*

1. B chooses distinct random primes **p** and **q**.
2. B computes $\mathbf{n} = (\mathbf{p}).(\mathbf{q})$ and $\phi = (\mathbf{p}-1).(\mathbf{q}-1)$.
3. B selects an encryption exponent **e** such that **e** and $\phi$ have no common factors.
4. B computes a decryption exponent $\mathbf{d} = 1/\mathbf{e} \mod \phi$.
5. B publishes both **e** and **n** as its public key and keeps **d** secret as its private key (**p**, **q** and $\phi$ are either destroyed or also kept secret)

*Message Transfer Phase*

6. A generates a message **m**.
7. A computes $\mathbf{m}^{\mathbf{e}} \mod \mathbf{n}$ and sends this to B.
8. B computes $(\mathbf{m}^{\mathbf{e}})^{\mathbf{d}} \mod \mathbf{n}$ to recover **m**.

The set up phase is carried out once whilst the message transfer phase is carried out for each message to be sent from A to B. In practice, the set up phase may be carried out on behalf of B by a certificate authority that provides a trustable certificate associating B to its

public key <e,n> and communicates **d** securely to B; the value of **e** is fixed for any particular domain.

It is often required to provide for control of message sending from A to B using a particular key pair. For example, A and B may initially be members of the same organisation with A sending messages to B using a public key for B that was certified or otherwise vouched for by the organisation as being associated with B; however, should B leave the organisation, it is desirable that the validity of B's public key be immediately revoked. One way of doing this is by the use of a revocation list that A must check each time it wants to send a message. A more reliable method is to use a mediated RSA method in which the decryption exponent **d** is split into two components, one held by B and the other held by a security mediator; in this case, both decryption exponent components must be applied to an encrypted message to decrypt it. This means that the security mediator must be contacted by B each time B wishes to decrypt a new encrypted message from A; the security mediator thus has control over which messages B decrypts and can therefore implement any desired control policy including, in the present example, preventing B decrypting messages after B has left the organisation.

However, it will generally be undesirable for the security mediator to have the ability to fully decrypt messages sent to B which implies that the security mediator must not have knowledge of B's decryption exponent component (or the data needed to compute it). Therefore, the security mediator must be separate from the entity generating the two decryption exponent components; since this latter entity clearly cannot be B (as B would then not need to go to the security mediator to decrypt a message), a separate key generation entity is needed with the result that most mediated RSA methods are four-party methods.

Figure 2 of the accompanying drawings depicts the operational steps carried out in a four-party mediated RSA method, the parties involved being a message sender A, a message recipient B, a security mediator SEM and a key generation center KGC each acting through a respective computing entity 10, 20, 30 and 40. The operational steps involved are:

*Initial Set Up Phase*

For each B, the KGC carries out steps 1 to 8

1. KGC chooses distinct random primes **p** and **q**.
2. KGC computes $\mathbf{n_B} = (\mathbf{p})x(\mathbf{q})$ and $\phi_B = (\mathbf{p}-1).(\mathbf{q}-1)$.
3. KGC selects an encryption exponent **e** (the same for all Bs) such that **e** and $\phi_B$ have no common factors.
4. KGC computes a decryption exponent $\mathbf{d} = 1/e \mod \phi_B$.
5. KGC chooses $\mathbf{d_U}$ (different for each B).
6. KGC computes $\mathbf{d_T} = (\mathbf{d} - \mathbf{d_U}) \mod \phi_B$.
7. KGC securely communicates $\mathbf{d_T}$ to the security mediator SEM and $\mathbf{d_U}$ to B.
8. KGC publishes both **e** and **n** as the public key for B.

*Message Transfer Phase*

9. A generates a message **m**.
10. A computes $\mathbf{m}^{\mathbf{e}} \mod \mathbf{n_B}$ and sends this to B which forwards it to the security mediator SEM.
11. SEM computes $\mathbf{x} = (\mathbf{m}^{\mathbf{e}})^{\mathbf{d_T}} \mod \mathbf{n_B}$ and returns it to B.
12. B receives **x** which is equivalent to $(\mathbf{m}^{\mathbf{e}})^{(\mathbf{d} - \mathbf{d_U})} \mod \mathbf{n_B}$.
13. B computes $\mathbf{x}^{\mathbf{d_U}} \mod \mathbf{n_B}$ to recover the message **m**.

B's decryption exponent component $\mathbf{d_U}$ can, of course, be generated by B or jointly by the KGC and B, provided both know its value (in other words $\mathbf{d_U}$ is a shared secret of B and the KGC). Unless the security mediator SEM only serves one recipient B, the security mediator will need to be provided with a recipient identifier in order to able to select which $\mathbf{d_T}$ and $\mathbf{n_B}$ to use in step 11. This recipient identifier can be one provided by the party passing it the encrypted message since it is not necessary for the security mediator to trust the recipient identifier – if the identifier does not identify the intended recipient of the message, then the message will not be even partially decrypted by application of the $\mathbf{d_T}$ retrieved using the identifier.

An inherent positive feature of the Figure 2 mediated RSA method is that the messages passing between B and the security mediator are encrypted. However, a drawback of the

method so far as B is concerned is that although there is apparent separation of the KGC and the security mediator which should ensure that messages to B cannot be read by the security mediator, in reality there is no guarantee for B that the KGC and the security mediator are not collaborating to read B's messages.

A recently proposed variant of the mediated RSA method provides an identifier-based cryptographic method; this variant is described in the paper "Identity based encryption using mediated RSA", D. Boneh, X. Ding and G. Tsudik, 3rd Workshop on Information Security Application, Jeju Island, Korea, Aug, 2002.

Identifier-Based Encryption (IBE) is an emerging cryptographic schema in which the encryption key used to encrypt a message is based on a sender-chosen string and public data, the corresponding decryption key being computed, potentially subsequent to message encryption, using the sender-chosen string and private data associated with the public data. Frequently, the sender-chosen string is a predetermined string that serves to "identify" the intended message recipient and this has given rise to the use of the label "identifier-based" or "identity-based" generally for these cryptographic methods. However, depending on the application to which such a cryptographic method is put, the sender-chosen string may serve a different purpose to that of identifying the intended recipient and, indeed, may be an arbitrary string having no other purpose than to form the basis of the encryption key. Accordingly, the use of the term "identifier-based" herein in relation to cryptographic methods and systems is to be understood simply as implying that the encryption key is based on a sender-chosen, cryptographically unconstrained, string whether or not the string serves to identify the intended recipient, and that the corresponding decryption key can be subsequently computed (though in certain applications it may be pre-computed). Furthermore, as used herein the term "string" is simply intended to imply an ordered series of bits regardless of their source.

In the identifier-based mediated RSA method described in the above-referenced paper, each potential recipient B has an associated predetermined identifier string $\mathbf{ID_B}$, such as an email address, that identifies the recipient. Thus, there exists a set of predetermined identifier strings $\mathbf{ID_B}$ which by their nature are generally known to A and to the key

generation center KGC. When A wishes to send a message to a particular recipient B, A chooses the relevant identifier string from the set of such strings and uses the chosen string to compute an encryption exponent. To effect its partial decrypt of the message, the security mediator SEM uses a decryption exponent component that the KGC has pre-computed for the recipient concerned using the known identifier string $\mathbf{ID_B}$ of that recipient. Figure 3 of the accompanying drawings depicts in more detail the operational steps of this identifier-based mediated RSA method, these operational steps being as follows:

*Initial Set Up Phase*

1. KGC chooses distinct random primes **p** and **q**. The primes p and q are specific to a particular domain and are not recipient dependent.
2. KGC computes $\mathbf{n} = (\mathbf{p}).(\mathbf{q})$ where **n** has a fixed value for the domain, this value being published in an appropriate certificate. KGC also computes $\phi = (\mathbf{p}\text{-}1).(\mathbf{q}\text{-}1)$.

For each B, the KGC carries out steps 3 to 8

3. KGC uses the identifier string $\mathbf{ID_B}$ of the particular recipient B concerned to compute a recipient-specific encryption exponent $\mathbf{e_B}$; the function $F$ used to compute $\mathbf{e_B}$ is typically a hash function. The exponent **e** and the value $\phi$ should have no common factors.
4. KGC computes a recipient-specific decryption exponent $\mathbf{d} = 1/\mathbf{e_B} \mod \phi$.
5. KGC chooses $\mathbf{d_U}$ (different for each B).
6. KGC computes a recipient-specific $\mathbf{d_T} = (\mathbf{d} - \mathbf{d_U}) \mod \phi$.
7. KGC securely communicates $\mathbf{d_T}$ to the security mediator SEM and $\mathbf{d_U}$ to B.
8. KGC publishes $\mathbf{ID_B}$ for B (only if not already known to message senders – where $\mathbf{ID_B}$ is B's email address, it typically would not be re-published by the KGC) .

*Message Transfer Phase*

9. A generates a message **m**.
10. A chooses the identifier string $\mathbf{ID_B}$ of the intended recipient and computes the corresponding encryption exponent $\mathbf{e_B}$ using the same function $F$ as used by the KGC (this function will have typically been incorporated in software provided to A's computing entity 10 for implementing the cryptographic method, but may be provided to A in any suitable manner including by distribution with **n**).

11. A computes $\mathbf{m}^{\mathbf{e}_B} \bmod \mathbf{n}$ and sends this to B which forwards it to the security mediator SEM.
12. SEM computes $\mathbf{x} = (\mathbf{m}^{\mathbf{e}_B})^{\mathbf{d}_T} \bmod \mathbf{n}$ and returns it to B.
13. B receives **x** which is equivalent to $(\mathbf{m}^{\mathbf{e}_B})^{(\mathbf{d} - \mathbf{d}_U)} \bmod \mathbf{n}$.
14. B computes $\mathbf{x}^{\mathbf{d}} \bmod \mathbf{n}$ to recover the message **m**.

This identifier-based mediated RSA method has the same features, positive and negative, mentioned above with respect to the mediated RSA method of Figure 2. Like the Figure 2 mediated RSA method, the identifier-based mediated RSA method of Figure 3 must keep the key generation center KGC independent of the security mediator if the latter is not to have access to the messages. As a result, the identifier strings used by A must generally be predetermined strings for which the KGC has already determined the corresponding decryption exponent component $\mathbf{d}_T$ to be used by the security mediator (the alternative of re-involving the KGC for each message to compute the $\mathbf{d}_T$ for use by the security mediator is unattractive in practical terms).

It should also be noted that the same message **m** must never be encrypted using two different encryption exponents as this would compromise the security of the method. As a consequence, the basic message data must normally be combined with random padding to form the message **m** to be sent.

It is an object of the present invention to provide improved mediated RSA cryptographic methods and systems.

Summary of the Invention

According to one aspect of the present invention, there is provided a mediated RSA cryptographic method in which a sender encrypts a message using an encryption exponent **e** and a public modulus **n**, and a recipient and a trusted authority cooperate with each other to decrypt the encrypted message by using respective components $\mathbf{d}_U$, $\mathbf{d}_T$ of a decryption exponent; a recipient, on receiving the encrypted message, carrying out first processing comprising a modulo-**n** blinding operation using a factor $\mathbf{r}^{\mathbf{e}}$ where **r** is a secret random

number, the resultant processed message being passed to the trusted authority which effects second processing comprising applying its decryption exponent component $\mathbf{d_T}$ to the message, and the resultant further-processed message being returned to the recipient which effects third processing comprising both cancelling the blinding and applying its decryption exponent component $\mathbf{d_U}$.

Blinding itself is a known technique (see, for example, "Blind signatures for untraceable payments" in Advances in Cryptology - D. Chaum, Crypto '82, pp. 199-203, Springer-Verlag, 1983); however, the present invention is based in part on the insight that application of blinding to four-party mediated RSA cryptographic methods permits these methods to become three-party in nature. More particularly, by using blinding it becomes possible to treat the key generation center and security mediator as a single entity as their separation is no longer necessary to ensure that a message is unreadable by the mediating entity.

A consequence of using blinding to prevent the trusted authority reading a message is that in identifier-based mediated RSA methods, where the sender chooses a string for which the decryption exponent component $\mathbf{d_T}$ has not been pre-computed it becomes possible for only a single entity, additional to the recipient, to be involved in the decryption process.

Whilst the method of the invention can be applied to situations where the trusted authority is set up to serve only one intended recipient, the trusted authority will typically serve multiple recipients each of which can be arranged to have its own associated decryption exponent component $\mathbf{d_U}$; in this case, the trusted authority needs to be provided, in relation to a message passed to it for processing, with a recipient identifier which the trusted authority uses to determine the appropriate decryption exponent component $\mathbf{d_T}$ for the second processing.

In a preferred embodiment, there is provided an identifier-based cryptographic method with the encryption exponent $\mathbf{e}$ being made a function of a string chosen by the sender. The trusted authority will typically then be arranged to use the string to calculate, subsequent to message encryption, the decryption exponent component $\mathbf{d_T}$ appropriate for the message,

the string either having been passed directly or indirectly from the sender to the trusted authority or, where the chosen string is one of a set of strings known to the trusted authority, looked up by the trusted authority on the basis of a string indicator provider from the sender. However, where the chosen string is one of a set of predetermined strings each specific to a particular intended recipient with its own value of $\mathbf{d_U}$, the decryption exponent component $\mathbf{d_T}$ can be pre-computed for each recipient and looked-up using the recipient identifier.

Advantageously, the string chosen by the sender comprises action information concerning actions to be taken by the trusted authority, the trusted authority using the action information in the string to carry out corresponding actions. Preferably, the action information specifies one or more conditions to be checked by the trusted authority, the second processing including the trusted authority checking these one or more conditions and only completing the second processing if the conditions are met. Typical conditions include a recipient-identity condition, conditions concerning other attributes of the intended recipient, and conditions unrelated to the intended recipient (such as a date or time condition).

In another embodiment, the encryption exponent **e** is fixed and the modulus **n** is specific to each of multiple recipients. In this case also, the trusted authority can be arranged either to store or calculate its corresponding decryption exponent components $\mathbf{d_T}$.

The present invention also encompasses systems, apparatus and computer program products for implementing the foregoing methods.

Brief Description of the Drawings

Embodiments of the invention will now be described, by way of non-limiting example, with reference to the accompanying diagrammatic drawings, in which:

. Figure 1 is a diagram illustrating the operational steps of the well-known basic RSA cryptographic method;

. Figure 2 is a diagram illustrating the operational steps of a prior art mediated RSA

cryptographic method;

. Figure 3 is a diagram illustrating the operational steps of a prior art identifier-based mediated RSA cryptographic method;

. Figure 4 is a diagram illustrating the operational steps of a blinded, identifier-based, mediated RSA cryptographic method forming a first embodiment of the invention;

. Figure 5 is a diagram illustrating the operational steps of a blinded, identifier-based, mediated RSA cryptographic method forming a second embodiment of the invention; and

. Figure 6 is a diagram illustrating the operational steps of a blinded mediated RSA cryptographic method forming a third embodiment of the invention.

Best Mode of Carrying Out the Invention

Three embodiments of the invention are described below, the first two embodiments concerning blinded, identifier-based (IB), mediated RSA methods and systems in which the value of the encryption exponent **e** is varied, and the third embodiment concerning a blinded, non-IB, mediated RSA method and system in which the value of **e** is kept constant and the value of the modulus **n** is made recipient specific.

**The identifier-based embodiments**

The identifier-based RSA cryptographic method and system forming the first embodiment of the invention is illustrated in Figure 4 and involves three parties, namely a message sender A acting through computing entity 10, a message receiver B acting through computing entity 20, and a trusted authority TA acting through computing entity 50. The computing entities 10, 20 and 50 are typically based around program-controlled processors though some or all of the cryptographic functions may be implemented in dedicated hardware. The entities 10, 20 and 50 inter-communicate, for example, via the internet or other computer network though it is also possible that two or all three entities actually reside on the same computing platform. For convenience, the following description is given in terms of the parties A, B and TA, it being understood that these parties act through their respective computing entities.

The RSA method of the first embodiment is similar to the prior art method illustrated in Figure 3 in that a predetermined identifier string $\mathbf{ID_B}$ of the intended message recipient B is used by the message sender A to compute the encryption exponent **e** for encrypting a message, and pre-computed decryption exponent components $\mathbf{d_U}$ and $\mathbf{d_T}$ are used to decrypt the encrypted message. However, the key generation center KGC and security mediator SEM of the Figure 3 arrangement are now treated as combined into the single trusted authority TA thereby giving a three-party method and system. Furthermore, in the Figure 4 method and system, the message recipient B blinds the encrypted message before passing it to the trusted authority for the latter to apply its decryption exponent component $\mathbf{d_T}$, the recipient B cancelling the blinding after receiving back the message processed by the trusted authority

A more detailed description of the operational steps involved in the Figure 4 method will now be given.

*Initial Set Up Phase*

This is the same as for the set up phase of the above-described identifier-based mediated RSA method depicted in Figure 3 with the trusted authority TA carrying out the same steps 1 to 8 as performed by the key generation center KGC; in particular, a domain-specific modulus **n** is chosen, values of $\mathbf{d_U}$ agreed, and values of $\mathbf{d_T}$ computed for each recipient identifier string $\mathbf{ID_B}$, these various values being distributed as required. However, because the trusted authority combines the roles of the key generation center and security mediator of the Figure 3 arrangement, there is no longer a need to securely communicate the computed values of the decryption exponent component $\mathbf{d_T}$, these values simply being kept secret by the trusted authority; in contrast, B now also needs to be provided with the predetermined function $F$ used to compute encryption exponents from the identifier strings $\mathbf{ID_B}$ and this can be done in the same way as the function was provided to A or in any other suitable manner.

*Message Transfer Phase*

Encryption of message by A

9. A generates a message **m**.

10. A chooses the identifier string $\mathbf{ID_B}$ of the intended recipient and computes the corresponding encryption exponent $\mathbf{e_B}$ using the same function $F$ as used by the trusted authority during the set up phase.

11. A computes $\mathbf{m}^{\mathbf{e_B}} \bmod \mathbf{n}$ and sends this to B.

Message Blinding by B

12. B chooses a secret random number r.

13. B computes $\mathbf{e_B}$ from the identifier string $\mathbf{ID_B}$ using the same function $F$ as used by the trusted authority during the set up phase. The identifier string $\mathbf{ID_B}$ may be passed to B by A along with the encrypted message or may be looked up by B using a recipient identifier provided by A (it being assumed that B has access to all identifier strings); alternatively, B can use its own identifier string on the basis that this will be the correct string to use if the message is intended for B (and if it isn't, use of the right or wrong string becomes irrelevant since B will not, in any event, be able to correctly decrypt the message as it does not have the correct $\mathbf{d_U}$).

14. B computes $\mathbf{r}^{\mathbf{e_B}} \bmod \mathbf{n}$.

15. B blinds the encrypted message by computing $(\mathbf{r}^{\mathbf{e_B}}).(\mathbf{m}^{\mathbf{e_B}}) \bmod \mathbf{n}$ and sends this to the trusted authority TA together with a recipient identifier (such as the string $\mathbf{ID_B}$).

Partial decryption by the trusted authority TA

16. The trusted authority TA uses the received recipient identifier to look up the value of $\mathbf{d_T}$ to apply and then computes $\mathbf{x} = ((\mathbf{r.m})^{\mathbf{e_B}})^{\mathbf{d_T}} \bmod \mathbf{n}$ and returns x to B.

Completion of decryption and cancellation of blinding by B

17. B receives x which is equivalent to $(\mathbf{r.m})^{\mathbf{e_B}(\mathbf{d} - \mathbf{d_U})} \bmod \mathbf{n}$.

18. B computes $\mathbf{y} = \mathbf{x}^{\mathbf{d_U}} \bmod \mathbf{n}$.

19. B computes $\mathbf{y/r} \bmod \mathbf{n}$ to recover the message m.

It will be appreciated that the blinding applied by B to the encrypted message before passing it to the trusted authority ensures that the latter cannot read the message even if it has retained B's value of $\mathbf{d_U}$ from the set up phase. The blinding, which involved a multiplication of the encrypted message by a factor $\mathbf{r^{e_B}}$ mod $\mathbf{n}$, is cancelled in steps 19 and 20 by a multiplication by a factor $\mathbf{r^{(ed_U - 1)}}$.

It may be noted that instead of recipient identifier strings $\mathbf{ID_B}$ being used as the basis for computing encryption exponents, any set of predetermined strings can be used with the corresponding values of $\mathbf{d_T}$ being computed during the set up phase (though now, assuming every string is potentially usable with every recipient, a respective value of $\mathbf{d_T}$ needs to be computed for every string/recipient combination as $\mathbf{d_T}$ is dependent both on the value of the string and on the value of $\mathbf{d_U}$). In this case, the sender A chooses an appropriate one of the predetermined strings when encrypting a message and the chosen string is passed from the sender to B and to the trusted authority to enable these entities to compute the correct value of $\mathbf{e}$ and to permit the trusted authority to look up the correct pre-computed value of $\mathbf{d_T}$ for the string having regard to the recipient concerned. One or both of the message recipient B and trusted authority can be arranged to store the set of predetermined strings and to retrieve the appropriate string from its store using a string indicator supplied to it in place of the string itself. The string indicator will generally have been initially provided by the sender A along with the encrypted message. It may also be noted that whilst the sender A could pass on the value of $\mathbf{e}$ for use by the other entities, the trusted authority should not rely on a value of $\mathbf{e}$ passed to it but should always compute $\mathbf{e}$ from the predetermined string used (this ensures that the sender has not chosen a specific value of $\mathbf{e}$ to gain cryptographic insights into private key data).

As already mentioned above, applying blinding to the encrypted message passed to the trusted authority, ensures that the latter cannot read the message. As a consequence, the trusted authority can be allowed to retain $\mathbf{d_U}$ after having used it in the set up phase to compute corresponding values of $\mathbf{d_T}$ for the predetermined strings. This opens up the possibility of the computation of the values of $\mathbf{d_T}$ being carried out after the set up phase;

in particular, the computation of a value of $\mathbf{d_T}$ can now be deferred until the time it is needed for use in decrypting a message. In turn, this gives rise to the significant advantage that the string used as the basis for the encryption key no longer needs to be a predetermined string but can be any string that the sender chooses to use, provided the string used is made known to the trusted authority.

The second embodiment of the invention, which is illustrated in Figure 5, provides an identifier-based mediated RSA method in which the string chosen by A as the basis for the encryption exponent can be any string as the corresponding value of $\mathbf{d_T}$ for any particular recipient is subsequently computed by the trusted authority. More particularly, the operational steps of the second embodiment are as follows:

*Initial Set Up Phase*

1. The trusted authority TA chooses distinct random primes $\mathbf{p} = 2p' + 1$ and $\mathbf{q} = 2q' + 1$ where both p' and q' are Sophie Germain primes. The primes p and q are specific to a particular domain/application/trusted-authority and are not recipient dependent.
2. TA computes $\mathbf{n} = (\mathbf{p}).(\mathbf{q})$ where **n** has a fixed value for the domain, this value being published in an appropriate certificate. TA also computes $\phi = (\mathbf{p}-1).(\mathbf{q}-1)$.
3. For each B, the TA and B share a secret $\mathbf{d_U}$ generated by one or other party or jointly.

*Message Transfer Phase*

Encryption of message by A

4. A generates a message **m**.
5. A chooses a string STR - this may be any string subject to any restrictions imposed, for example, by a particular application or by the trusted authority.
6. A applies the predetermined function *F* to the string STR to compute a corresponding encryption exponent **e**, the function being such that **e** is odd.
7. A computes $\mathbf{m}^{\mathbf{e}}$ mod **n** and sends this to B along with the string STR.

Message Blinding by B

8. B chooses a secret random number r.
9. B computes **e** from the string STR using the predetermined function *F*.
10. B computes $\mathbf{r}^{\mathbf{e}}$ mod **n**.
11. B computes $(\mathbf{r}^{\mathbf{e}}).(\mathbf{m}^{\mathbf{e}})$ mod **n** and sends this to the trusted authority TA together with the string STR and a recipient identifier.

Partial decryption by the trusted authority TA

12. B computes **e** from the string STR using the predetermined function *F*.
13. TA computes decryption exponent $\mathbf{d} = 1/\mathbf{e} \mod \phi$.
14. TA computes $\mathbf{d_T} = (\mathbf{d} - \mathbf{d_U}) \mod \phi$.
15. TA then computes $\mathbf{x} = ((\mathbf{r.m})^{\mathbf{e}})^{\mathbf{d_T}} \mod \mathbf{n}$ and returns **x** to B.

Completion of decryption and cancellation of blinding by B

16. B receives **x** which is equivalent to $(\mathbf{r.m})^{\mathbf{e}(\mathbf{d} - \mathbf{d_U})} \mod \mathbf{n}$.
17. B computes $\mathbf{y} = \mathbf{x}^{\mathbf{d_U}} \mod \mathbf{n}$.
18. B computes $\mathbf{y/r} \mod \mathbf{n}$ to recover the message **m**.

The Figure 5 blinded, identifier-based, mediated RSA method thus ensures that the trusted authority cannot read the message **m** whilst guaranteeing its involvement in message decryption. In addition, any string STR can be used and the trusted authority is not required to store any data other than the values of **p** and **q** (and/or their derivatives **n** and $\phi$) and the or each value of $\mathbf{d_U}$.

As regards the string STR chosen by the sender, as already indicated, this string may be any string. The string can be based on a character string, a serialised image bit map, a digitised sound, or any other data including data input by the sender using any suitable input device such as a keyboard or keypad. However, in many cases restrictions will be placed on the strings selectable by the sender. For example, the string may be required to conform to a predetermined set of rules with regard to its formatting and/or content (e.g. the string STR

may be required to comply with a particular XML schema); alternatively, the sender may be required to select a string from a set of predetermined strings provided by the trusted authority or by another party. In this latter case, the predetermined set of strings can be stored by the trusted authority and/or B and retrieved against a string indicator provider by the sender A, the retrieved string then being used in the computation of **e**.

Generally (though not necessarily), the string STR is used to convey to the trusted authority information concerning actions to be taken by the trusted authority when it receives the encrypted message for decryption. If a recipient B changes the information in the string before passing it to the trusted authority, the string will no longer be usable to compute the correct decryption exponent $\mathbf{d}_T$ in steps 12 to 14 of Figure 5.

The information in the string STR may relate to actions to be taken by the trusted authority that do not affect message decryption – for example, the trusted authority TA may be required to send a message to the message sender A at the time the TA decrypts the message concerned. However, the information in the string STR will frequently specify one or more conditions to be checked by the trusted authority as being satisfied before the trusted authority partially decrypts the related encrypted message (or before returning the corresponding partially decrypted message to the recipient B concerned).

For example, the string STR may comprise a recipient identity condition identifying a specific intended message recipient; in this case, the trusted authority carries out an authentication process with the recipient B presenting the related message for decryption to check that the recipient concerned meets the recipient-identity condition.

Rather than identifying an intended recipient as a particular individual, the string STR may comprise one or more conditions specifying one or more non-identity attributes that the recipient must possess; for example, a condition may specify that a recipient must have a certain credit rating. Again, it is the responsibility of the trusted authority to check out this condition before producing the decrypted message for a recipient presenting the encrypted message for decryption.

The string STR may additionally or alternatively comprise one or more conditions unrelated to an attribute of the intended recipient; for example, a condition may be included that the message concerned is not to be decrypted before a particular date or time.

Whatever the conditions relate to, the string STR may directly set out the or each condition or may comprises one or more condition identifiers specifying corresponding predetermined condition known to the trusted authority (in the latter case, the trusted authority uses the or each condition identifier to look up the corresponding condition to be checked).

In the Figure 5 embodiment, the value of the public modulus **n** and of the corresponding private data **p,q** (or $\phi$) held by the trusted authority is assumed to be fixed for the domain/application/trusted-authority concerned. However, it is possible for multiple different values of the modulus **n** and the corresponding private data to be in use together. For example, there may be multiple groups of recipients each of which has associated value of **n** and of the corresponding private data. In the extreme, each recipient B has its own associated values of **n** and **p,q** (or $\phi$). Of course, where there are multiple values of **n** and **p,q** (or $\phi$) in use, the trusted authority needs to be provided with an indication of the values to be used for any particular message; for example, a group or recipient indicator can be included in the string STR or provided by the recipient B presenting the encrypted message for decryption.

**Non IB embodiment**

The third embodiment depicted in Figure 6 concerns a blinded, non-IB, mediated RSA method and system in which the value of **e** is kept constant and the value of the modulus **n** is made recipient specific; this embodiment thus has similarities with the prior art four-party mediated RSA method of Figure 2. However, the Figure 6 embodiment is a three-party method combining the key generation center and security mediator of Figure 2 into a single trusted authority entity. The operational steps of the third embodiment are as follows:

*Initial Set Up Phase*

This is the same as for the set up phase of the prior art mediated RSA method depicted in Figure 2 with the trusted authority TA carrying out the steps 1 to 8 performed by the key generation center KGC (with the result that no communication of $\mathbf{d_T}$ is required). B is now also provided with the encryption exponent **e**.

*Message Transfer Phase*

Encryption of message by A

9. A generates a message **m**.
10. A computes $\mathbf{m^e}$ mod $\mathbf{n_B}$ and sends this to B.

Message Blinding by B

11. B chooses a secret random number r.
12. B computes $\mathbf{r^e}$ mod $\mathbf{n_B}$ using it's own value of $\mathbf{n_B}$.
13. B computes $(\mathbf{r^e}).(\mathbf{m^e})$ mod $\mathbf{n_B}$ again using it's own value of $\mathbf{n_B}$ and sends the result to the trusted authority TA together with a recipient identifier (such as $\mathbf{n_B}$).

Partial decryption by the trusted authority TA

14. The trusted authority TA uses the received recipient identifier to look up the value of $\mathbf{d_T}$ (and $\mathbf{n_B}$ if not supplied) to use and computes $\mathbf{x} = ((\mathbf{r.m})^{\mathbf{e}})^{\mathbf{d_T}}$ mod **n**; TA then returns the computed value of x to B.

Completion of decryption and cancellation of blinding by B

15. B receives **x** which is equivalent to $(\mathbf{r.m})^{\mathbf{e(d - d_U)}}$ mod $\mathbf{n_B}$.
16. B computes $\mathbf{y} = \mathbf{x}^{\mathbf{d_U}}$ mod $\mathbf{n_B}$.
17. B computes **y/r** mod $\mathbf{n_B}$ to recover the message **m**.

Again, because of the blinding applied by B, the trusted authority is unable to read the message presented to it by B.

**General**

As is the case with all mediated RSA methods, in the embodiments of the invention described herein, the trusted authority TA will typically perform a control function (over and above that associated with implementing any conditions contained in the string STR) for ensuring that the recipient B presenting the trusted authority with a message for partial decryption, is only serviced if entitled to receive such a service; thus, for example, the trusted authority can provide for immediate implementation of a revocation list.

It may be noted that a consequence of the recipient B applying blinding to the encrypted message sent to the trusted authority is that it is no longer essential for the recipient's decryption exponent component $\mathbf{d}_U$ to be kept secret to ensure that a third party cannot read the message. However, keeping $\mathbf{d}_U$ secret has the benefit of ensuring that only the intended recipient can correctly decrypt the message thereby relieving the trusted authority of the need to check that the recipient B presenting it with the encrypted message corresponds to an intended recipient (as may have been indicated to the trusted authority, for example, in the string STR in the case of the Figure 5 embodiment).

As is well known, in RSA methods the encryption exponent **e** must have no common factors with **(p-1).(q-1).** This can be checked by the trusted authority where **e** is known in advance to the trusted authority; however, in the identifier-based mediated RSA embodiments of the invention **e** may not be known to the trusted authority in advance of its use - for example, in the Figure 5 embodiment the encryption exponent **e** may be based on a string created by the sender. In order to meet the requirement that the encryption exponent **e** have no common factors with **(p-1).(q-1),** where the trusted authority does not know **e** in advance, the following constraints (already stated in the description of the Figure 5 embodiment) can be imposed:

- the function $F$ used to generate the encryption exponent is such that **e** is always odd; and
- $\mathbf{p} = (2\mathbf{p}' + 1)$ and $\mathbf{q} = (2\mathbf{q}' + 1)$ where **p'** and **q'** are Sophie Germain primes.

These constraints together serve to ensure, with a very high probability, that the encryption exponent **e** and **(p-1).(q-1)** will have no common factors.

Whilst the above-described embodiments are adequate in some environments, for most environments certain constraints need to be applied to remove their vulnerability to a number of attacks.

**Traffic Analysis:** If the same encrypted message is seen twice, then it is likely that it is the same message being encrypted with the same key and transmitted. This gives information to the attacker. The cure is to use random padding to ensure that the same message is never encrypted twice. The basic message content is thus combined with random padding and a message-content length indicator to form the message **m** to be encrypted.

**Active Attacker:** In the described embodiments, B passes $(\mathbf{r.m})^{\mathbf{e}}$ mod **n** to the trusted authority. A third party intercepting this message could compute:

$$(\mathbf{newm}^{\mathbf{e}}/\mathbf{m}^{\mathbf{e}}).(\mathbf{r.m})^{\mathbf{e}} \bmod \mathbf{n} = (\mathbf{r.newm}^{\mathbf{e}}) \bmod \mathbf{n}$$

thus changing the message **m** to **newm**. The channel between B and TA should therefore be able to detect any attempt to modify the message.

**Common Modulus Attack:** With RSA methods it is accepted that one should never encrypt the same message multiple times with different exponents that are coprime, since an attacker could then use the Extended Euclidean Algorithm to recover the original message. The embodiments of Figures 4 and 5 are vulnerable to this attack; however, various solutions are available:

- Use random padding of the message, as described above, to ensure that the same message is never encrypted twice.
- Ensure that the same message content is never re-sent - whilst this is possible to do in theory (for example, by storing all sent messages and checking any new message against the stored messages) in reality this solution is only practical in limited situations.
- Ensure that the exponents are never coprime (that is, values of **e** derived from different strings having a common divisor greater than one). This can be achieved, for example,

by making all exponents a multiple of 3; thus e can be derived from the string STR using a hash function # for which #(STR) ≡ 3 mod 6 - in other words:

$$e=3(\,2(\#(STR))+1)$$

More generally, successive values of e can be derived as:

$$e = z(\,2(\#(STR))+1)$$

where z is an odd integer ≥ 3, this value being fixed (that is, the same value is used for each successive calculation of e).

Another point to note regarding reducing vulnerability to cryptographic attacks is that the size of the message should, preferably, be similar to the value of the modulus n and this can be achieved by always adding an appropriate amount of random padding to the message content. Thus, for example, where the "message" is, in fact, a symmetric cryptographic key for encoding/decoding subsequent exchanges, the message can be padded by any suitable padding scheme such as OAEP (M. Bellare and P. Rogaway. Optimal Asymmetric Encryption - How to Encrypt with RSA. In Advances in Cryptology-Eurocrypt '94, pp. 92-111, Springer-Verlag, 1994).

With respect to the form of the blinding applied by the recipient B, in the described embodiments this has involved a modulo-**n** multiplication of the encrypted message by $\mathbf{r}^{\mathbf{e}}$, the blinding being subsequently cancelled by a modulo-**n** division of the message returned by the trusted authority by $\mathbf{r}^{(ed_U - 1)}$. It will be appreciated by persons skilled in the art that the factor $\mathbf{r}^{\mathbf{e}}$ mod n can be applied in other ways to blind the encrypted message. For example, the blinding operation can comprise a modulo-**n** division of the encrypted message by $\mathbf{r}^{\mathbf{e}}$ (that is, a modulo-n multiplication by $\mathbf{r}^{-\mathbf{e}}$ ) with the blinding being subsequently cancelled by a modulo-**n** multiplication of the blinded decrypted message by $\mathbf{r}^{(1 - ed_U)}$. It will also be appreciated that cancellation of the blinding operation following return of the partially-decrypted message from the trusted authority, can be effected before, jointly with, or after application of the recipient's decryption exponent component $\mathbf{d_U}$. As regards the random number r, this should have a large value and should be generated by a

cryptographically-strong random number generator. The blinding operation and its subsequent cancellation are totally transparent to the trusted authority.

As is generally the case with mediated RSA methods, in all the embodiments described herein, unless the trusted authority only serves one recipient B, the trusted authority will need to be provided with an identifier, generally a recipient identifier, in order to able to determine, by computation or look up, the correct value of $\mathbf{d_T}$ to use in carrying out its partial message decryption. Such a recipient identifier will typically be one of:

- an identifier provided by the recipient B that presents the message to the trusted authority;
- the value of the encryption exponent **e** used by the sender or the value of all or part of a string upon which that encryption exponent is based, in cases where a different respective said value is associated with each of multiple recipients;
- the value of the modulus **n** used by the sender where a different respective said value is associated with each of multiple recipients.

Embodiments are possible in which the value of $\mathbf{d_U}$ is made the same for all recipients rather than being a recipient-specific secret. Thus, the Figure 5 embodiment and its variants, the value of $\mathbf{d_U}$ can be made the same for all recipients and the appropriate value of $\mathbf{d_T}$ is calculated using this fixed value of $\mathbf{d_U}$. The fixed value of $\mathbf{d_U}$ can, for example, be 1 so that the calculation of $\mathbf{d_T}$ becomes $\mathbf{d_T} = (\mathbf{d}\text{-}1) \bmod \phi$; advantageously, where the STR passed to the trusted authority includes conditions to be checked (such as the identity of recipient B), the condition-checking process is arranged to output a value of 0 or 1 for fail or pass and this value is then subtracted (mod $\phi$) from d to produce $\mathbf{d_T}$ whereby the correct value of $\mathbf{d_T}$ is only produced when the conditions specified in STR have been met (alternatively, if the output from the condition-checking process is 0, $\mathbf{d_T}$ is not determined). Making the value of $\mathbf{d_U}$ fixed for all recipients can also be done in respect of the embodiments of Figures 4 and 6. It will be appreciated that where the value of $\mathbf{d_U}$ is fixed, the trust authority can no longer rely on $\mathbf{d_U}$ to ensure that only the intended recipient can complete the decryption process; the trust authority should therefore check that the identity of the recipient requesting the partial decryption corresponds to that indicated either in the identity string STR (embodiments of Figures 4 and 5) or by a value of n indicated by the

recipient requesting partial decryption (Figure 6 embodiment and also usable for the Figure 5 variant where the value of n is recipient dependent).

In certain situations it may be required that a message should only be decryptable with the cooperation of multiple trusted authorities. One way of doing this with mediated RSA methods is to sub-divide the decryption exponent component $\mathbf{d_T}$ into multiple sub-components each of which is held (or computable) by a respective trusted-authority entity (in effect, the trusted authority of the described embodiments is divided into multiple sub-authorities). In this case, the recipient B must go to each trusted-authority entity to get a message decrypted, each such entity applying its sub-component of $\mathbf{d_T}$ to the message to be decrypted.

For the identifier-based mediated RSA methods, another approach is possible and involves each trusted authority having its own associated public modulus $\mathbf{n}$ and private data. Consider, for example, the situation where the sender wishes to impose multiple conditions but no single trusted authority is competent to check all conditions – in this case, different trusted authorities can be used to check different conditions. In one implementation, the sender organizes the message content as a number of data sets (say k data sets) by using Shamir's secret sharing scheme and then encrypts each data set using an associated string STR (for example, specifying a respective condition to be checked) and the public modulus of a respective one of the trusted authorities; in order to retrieve the message, a recipient B has to go to all of the trusted authorities in order to decrypt all of the data sets because any k-1 data sets or less cannot disclose any of the message contents.

## CLAIMS

1. A mediated RSA cryptographic method in which a sender encrypts a message using an encryption exponent **e** and a public modulus **n**, and a recipient and a trusted authority cooperate with each other to decrypt the encrypted message by using respective components $\mathbf{d_U}$, $\mathbf{d_T}$ of a decryption exponent; the recipient, on receiving the encrypted message, carrying out first processing comprising a modulo-**n** blinding operation using a factor $\mathbf{r^e}$ where **r** is a secret random number, the resultant processed message being passed to the trusted authority which effects second processing comprising applying its decryption exponent component $\mathbf{d_T}$ to the message, and the resultant further-processed message being returned to the recipient which effects third processing comprising both applying its decryption exponent component $\mathbf{d_U}$ and cancelling the blinding.

2. A cryptographic method according to claim 1, wherein:

- the blinding operation comprises a modulo-**n** multiplication of the encrypted message by $\mathbf{r^e}$; and
- in said third processing the blinding is cancelled by a modulo-**n** multiplication of the blinded decrypted message by $\mathbf{r^{(ed_U-1)}}$.

3. A cryptographic method according to claim 1, wherein:

- the blinding operation comprises a modulo-**n** division of the encrypted message by $\mathbf{r^e}$; and
- in said third processing the blinding is cancelled by a modulo-**n** multiplication of the blinded decrypted message by $\mathbf{r^{(1-ed_U)}}$.

4. A cryptographic method according to claim 1, wherein the message comprises a content portion, random padding and a content length indicator.

5. A cryptographic method according to claim 1, wherein the blinded message is passed from the recipient to the trusted authority over a channel arranged to detect any modification of the blinded message.

6. A cryptographic method according to claim 1, wherein the trusted authority serves multiple recipients each of which has its own associated decryption exponent component $\mathbf{d_U}$; the trusted authority being provided, in relation to a said message passed to it for processing, with a recipient identifier which the trusted authority uses to determine the appropriate decryption exponent component $\mathbf{d_T}$ for said second processing.

7. A cryptographic method according to claim 6, wherein said recipient identifier is one of:

- an identifier provided by the recipient passing the message to the trusted authority;
- the value of the encryption exponent **e** used by the sender or the value of all or part of a string upon which that encryption exponent is based, where a different respective said value is associated with each of said multiple recipients;
- the value of the modulus **n** used by the sender where a different respective said value is associated with each of said multiple recipients.

8. A cryptographic method according to claim 1, wherein said encryption exponent **e** is a function of a string chosen by the sender.

9. A cryptographic method according to claim 8, wherein said function is such that **e** is odd, and wherein the public modulus **n** is the product of two distinct random primes:

$$p = (2p' + 1)$$

$$q = (2q' + 1)$$

where p' and q' are Sophie Germain primes, p and q being private to the trusted authority.

10. A cryptographic method according to claim 9, wherein said function is such that the values of **e** derived from different strings have a common divisor greater than one.

11. A cryptographic method according to claim 9, wherein said function takes the form:

$$e = z(\ 2(\#(\text{sender-chosen string})) + 1)$$

where # is a hash function and z is an odd integer greater than or equal to 3, the same value of z being used for successive determinations of e.

**12.** A cryptographic method according to claim 9, wherein said function is a hash function where hash(sender-chosen string) ≡ 3 mod 6.

**13.** A cryptographic method according to claim 1, wherein:

- said encryption exponent **e** is a function of a string chosen by the sender, and
- the trusted authority serves multiple recipients each of which has its own associated decryption exponent component $\mathbf{d_U}$;

the trusted authority being provided, in relation to a said message passed to it for processing, with a recipient identifier which the trusted authority uses to determine, for the string chosen by the sender, the appropriate decryption exponent component $\mathbf{d_T}$ to use for said second processing.

**14.** A cryptographic method according to claim 13, wherein:

- the trusted authority stores the recipient decryption exponent components $\mathbf{d_U}$ of said multiple recipients;
- the sender-chosen string used in forming the encryption exponent **e** for encrypting a said message, is passed to the trusted authority in association with the message; and
- the trusted authority uses the said recipient identifier relating to the message to look up the corresponding recipient decryption exponent component $\mathbf{d_U}$ which it then uses, together with said string and private data associated with said modulus **n**, to compute the decryption exponent component $\mathbf{d_T}$ to be used in said second processing.

**15.** A cryptographic method according to claim 14, wherein the sender-chosen string comprises information concerning actions to be taken by the trusted authority, the trusted authority using the information in the string to carry out corresponding actions.

**16.** A cryptographic method according to claim 15, wherein said information specifies one or more conditions to be checked by the trusted authority, the trusted authority, in carrying out said second processing, checking said one or more conditions and only completing the

second processing or only passing the resultant further-processed message to the recipient, if satisfied that said one or more conditions are met.

**17.** A cryptographic method according to claim 14, wherein the modulus **n** and the associated private data are specific to the trusted authority.

**18.** A cryptographic method according to claim 14, wherein the modulus **n** and the associated private data are specific to each of said multiple recipients and at least these private datas are stored by the trusted authority, the trusted authority further using the recipient identifier to look up the corresponding private data to be used in computing the decryption exponent component $\mathbf{d_T}$.

**19.** A cryptographic method according to claim 13, wherein:

- the string chosen by the sender is chosen from a set of predetermined strings;
- the trusted authority stores both the recipient decryption exponent components $\mathbf{d_U}$ of said multiple recipients, and said set of predetermined strings;
- an indicator of the sender-chosen string used in relation to said message is passed, in associated with the message, to the trusted authority, the trusted authority using this indicator to look up the corresponding stored string; and
- the trusted authority uses the said recipient identifier relating to the message to look up the corresponding recipient decryption exponent component $\mathbf{d_U}$ which it then uses, together with the looked-up string and private data associated with said modulus **n**, to compute the decryption exponent component $\mathbf{d_T}$ to be used in said second processing.

**20.** A cryptographic method according to claim 19, wherein said set of predetermined strings comprises a respective string for each of said multiple recipients, said indicator of the sender-chosen string being formed by the recipient indicator.

**21.** A cryptographic method according to claim 20, wherein said information specifies one or more conditions to be checked by the trusted authority, the trusted authority, in carrying out said second processing, checking said one or more conditions and only completing the

second processing or only passing the resultant further-processed message to the recipient, if satisfied that said one or more conditions are met.

**22.** A cryptographic method according to claim 19, wherein the trusted authority stores said set of predetermined strings and at least some of the strings comprise information concerning actions to be taken by the trusted authority, the trusted authority using this information where present in a said looked-up string to carry out corresponding actions.

**23.** A cryptographic method according to claim 19, wherein the modulus **n** and the associated private data are specific to the trusted authority.

**24.** A cryptographic method according to claim 19, wherein the modulus **n** and the associated private data are specific to each of said multiple recipients and at least these private datas are stored by the trusted authority, the trusted authority further using the recipient identifier to look up the corresponding private data to be used in computing the decryption exponent component $\mathbf{d_T}$.

**25.** A cryptographic method according to claim 13, wherein the string chosen by the sender is chosen from a set of predetermined strings comprising a different string for each of said multiple recipients, the trusted authority storing its corresponding decryption exponent component $\mathbf{d_T}$ for each recipient; and the trusted authority using said recipient identifier relating to a message passed to it for processing to look up its corresponding decryption exponent component $\mathbf{d_T}$ to be used in said second processing.

**26.** A cryptographic method according to claim 25, wherein at least some of the strings comprise information concerning actions to be taken by the trusted authority, the trusted authority using the recipient identifier to look up the corresponding string and using said information, where present in a looked-up string, to carry out corresponding actions.

**27.** A cryptographic method according to claim 26, wherein said information specifies one or more conditions to be checked by the trusted authority, the trusted authority, in carrying out said second processing, checking said one or more conditions and only completing the

second processing or only passing the resultant further-processed message to the recipient, if satisfied that said one or more conditions are met.

**28.** A cryptographic method according to claim 1, wherein:

- said encryption exponent **e** is a function of a string chosen by the sender, and
- the trusted authority serves multiple recipients with the value of the decryption exponent component $d_U$ associated with each recipient being the same;

the trusted authority being provided, in relation to a said message passed to it for processing, with a recipient identifier, formed by all or part of said string, against which the trusted authority checks the identity of the recipient providing the message for processing; and, at least where this recipient-identity check is passed, the trusted authority using the string, the value of $d_U$, and private data associated with said modulus **n**, to compute the appropriate decryption exponent component $\mathbf{d_T}$ to use for said second processing.

**29.** A cryptographic method according to claim 15, wherein said string, in addition to including said recipient identifier, specifies one or more conditions to be checked by the trusted authority, the trusted authority, in carrying out said second processing, checking said one or more conditions and only completing the second processing or only passing the resultant further-processed message to the recipient, if satisfied that said one or more conditions are met.

**30.** A cryptographic method according to claim 28, wherein the modulus **n** and the associated private data are specific to the trusted authority.

**31.** A cryptographic method according to claim 28, wherein the modulus **n** and the associated private data are specific to each of said multiple recipients and at least these private datas are stored by the trusted authority, the trusted authority further using the recipient identifier to look up the corresponding private data to be used in computing the decryption exponent component $\mathbf{d_T}$.

**32.** A cryptographic method according to claim 1, wherein:

- said encryption exponent **e** is a function of a string chosen by the sender,

- the trusted authority serves multiple recipients with the value of the decryption exponent component $d_U$ associated with each recipient being the same, and
- the modulus **n**, and associated private data known to the trusted authority, are specific to each of said multiple recipients and at least these private datas are stored by the trusted authority;

the trusted authority being provided, in relation to a said message passed to it for processing, with a recipient identifier, in the form of said modulus, against which the trusted authority checks the identity of the recipient providing the message for processing; and, at least where this recipient-identity check is passed, the trusted authority using the string, the value of $d_U$, and the private data associated with the modulus **n** provided as the recipient identifier, to compute the appropriate decryption exponent component $\mathbf{d_T}$ to use for said second processing.

**33.** A cryptographic method according to claim 32, wherein the sender-chosen string comprises information concerning actions to be taken by the trusted authority, the trusted authority using the information in the string to carry out corresponding actions.

**34.** A cryptographic method according to claim 33, wherein said information specifies one or more conditions to be checked by the trusted authority, the trusted authority, in carrying out said second processing, checking said one or more conditions and only completing the second processing or only passing the resultant further-processed message to the recipient, if satisfied that said one or more conditions are met.

**35.** A cryptographic method according to claim 1, wherein:

- the trusted authority serves multiple recipients and said encryption exponent **e** is a function of a string chosen by the sender from a set of predetermined strings comprising a different string for each of said multiple recipients, and
- the value of the decryption exponent component $d_U$ associated with each recipient is the same;

the trusted authority being provided, in relation to a said message passed to it for processing, with a recipient identifier, formed by said string, against which the trusted authority checks the identity of the recipient providing the message for processing; and, at

least where this recipient-identity check is passed, the trusted authority using the string to look up its corresponding decryption exponent component $\mathbf{d_T}$ to be used in said second processing.

**36.** A cryptographic method according to claim 1, wherein:

- said encryption exponent **e** is fixed,
- the trusted authority serves multiple recipients with the value of the modulus **n** being specific to each recipient, and
- the value of the decryption exponent component $\mathbf{d_U}$ is specific to each said recipient and the trusted authority stores the corresponding decryption exponent component $\mathbf{d_T}$ for each recipient;

the trusted authority being provided, in relation to a said message passed to it for processing, with a recipient identifier and the trusted authority using the said recipient identifier to look up the corresponding decryption exponent component $\mathbf{d_T}$ to be used in said second processing.

**37.** A cryptographic method according to claim 16, wherein:

- said encryption exponent **e** is fixed,
- the trusted authority serves multiple recipients with the value of the modulus **n**, and of associated private data known to the trusted authority, being specific to each recipient, at least these private datas being stored by the trusted authority, and
- the value of the decryption exponent component $\mathbf{d_U}$ is specific to each said recipient with these values being stored by the trusted authority;

the trusted authority being provided, in relation to a said message passed to it for processing, with a recipient identifier and the trusted authority using the said recipient identifier to look up the corresponding recipient decryption exponent component $\mathbf{d_U}$ and private data which it then uses, together with said encryption exponent, to compute the decryption exponent component $\mathbf{d_T}$ to be used in said second processing.

**38.** A cryptographic method according to claim 1, wherein:

- said encryption exponent **e** is fixed,

- the trusted authority serves multiple recipients with the value of the modulus **n** being specific to each recipient,
- the value of the decryption exponent component $d_U$ associated with each recipient is the same, and
- the trusted authority stores the appropriate decryption exponent component $\mathbf{d_T}$ for each recipient;

the trusted authority being provided, in relation to a said message passed to it for processing, with a recipient identifier, in the form of said modulus **n**, against which the trusted authority checks the identity of the recipient providing the message for processing; and, at least where this recipient-identity check is passed, the trusted authority using the recipient identifier to look up the appropriate decryption exponent component $\mathbf{d_T}$ to use for said second processing.

**39.** A cryptographic method according to claim 1, wherein:

- said encryption exponent **e** is fixed,
- the trusted authority serves multiple recipients with the value of the modulus **n**, and of associated private data known to the trusted authority, being specific to each recipient, at least these private datas being stored by the trusted authority, and
- the value of the decryption exponent component $d_U$ associated with each recipient is the same;

the trusted authority being provided, in relation to a said message passed to it for processing, with a recipient identifier in the form of said modulus, against which the trusted authority checks the identity of the recipient providing the message for processing; and, at least where this recipient-identity check is passed, the trusted authority using the recipient identifier to look up the corresponding said private data which it then uses, together with said encryption exponent and the decryption exponent component $d_U$, to compute the decryption exponent component $\mathbf{d_T}$ to be used in said second processing.

**40.** A cryptographic system for carrying out the cryptographic method of claim 1.

**41.** Cryptographic apparatus for carrying out the operations effected by the recipient in the cryptographic method of claim 1.

**42**. A computer program product for conditioning programmable computing apparatus to carry out the operations effected by the recipient in the cryptographic method of claim 1.

**Application No:** GB0412786.6 **Examiner:** Mr Adam Tucker

**Claims searched:** 1-42 **Date of search:** 6 October 2004

# Patents Act 1977: Search Report under Section 17

**Documents considered to be relevant:**

| Category | Relevant to claims | Identity of document and passage or figure of particular relevance |
|---|---|---|
| X,P | 1 at least | WO03/073713 A1 (University of Hong Kong) See in particular the abstract |
| Y | 1 at least | US6275936 B1 (Kyojima et al.) See in particular the background of the invention and col 8 |
| Y | 1 at least | http://pollux.usc.edu/~xuhuad/publications/wisa.pdf, "Identity-based mediated RSA", D. Boneh, X. Ding & G. Tsudik, 3rd International Workshop on Information and Security Applications (WISA'02), Jeju Island, Korea, 2002 |
| A | - | WO03/017559 A2 (Leland Stanford Junior University) See in particular the abstract |
| A | - | http://www.hpl.hp.com/techreports/2003/HPL-2003-101.pdf, "IBE applied to privacy and identity management", Marco Casassa Mont and Pete Bramhall, HP Labs Technical Reports, last modified 02/06/2003 |
| A | - | "A blind signature scheme based on ElGamal signature", Mohammed, E.; Emarah, A.E.; El-Shennawy, K., EUROCOMM 2000, Information Systems for Enhanced Public Safety and Security, IEEE/AFCEA , 17 May 2000, pp 51-53 |
| A | - | http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C82/199.PDF, "Blind signatures for untraceable payments", Advances in Cryptology, Crypto >82, D. Chaum, pp199-203 |

Categories:

| | | | |
|---|---|---|---|
| X | Document indicating lack of novelty or inventive step | A | Document indicating technological background and/or state of the art. |
| Y | Document indicating lack of inventive step if combined with one or more other documents of same category. | P | Document published on or after the declared priority date but before the filing date of this invention. |
| & | Member of the same patent family | E | Patent document published on or after, but with priority date earlier than, the filing date of this application. |

**Field of Search:**

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[W] :

H4P

Worldwide search of patent documents classified in the following areas of the IPC[07]

G07F; H04L

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC, PAJ, INSPEC and selected internet sites